EXHIBIT 7

4526 ACCESS TO COMPUTER NETWORK FOR USE IN INSTRUCTION

The Board of Education is committed to optimizing student learning and teaching. The Board considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in district classrooms for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

The district provides faculty, staff and students with access to the district's electronic network. This network includes Internet access (including through its wireless network), computer services, email, videoconferencing, computer equipment and related equipment for educational purposes. The purpose of this network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world, to gain the ability to create new technological tools and content, and to provide faculty and staff with the resources to provide instruction to students and to perform their duties and responsibilities for the district.

As part of the district's instructional program, students (and their parents/guardians) and staff may be provided with access to and use of accounts from an outside internet educational resource provider through which access will be provided to that provider's services. The district shall comply with all contractual and other requirements related to the use of such services by its students (and their parents/guardians) and staff, and shall ensure that all such users execute any consent or authorization forms required for such use.

This document contains the rules and procedures relating to the acceptable use of the district's electronic network.

Acceptable network use by district students and staff includes:

- Creation of files, projects, videos, web pages, podcasts and other media using network resources in support of educational research;
- Creation of new programs, applications or other code for educational purposes, under appropriate faculty supervision;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- The use of online applications for learning that support the educational process in accordance with applicable district policies;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all District policies and guidelines;
- Connection of staff personal electronic/digital devices in accordance with applicable district policies.

Unacceptable network use by district students and staff includes but is not limited to:

- Use for personal gain, commercial solicitation and compensation of any kind;

- Use that may result in liability or cost incurred by the district;
- Downloading, installation and use of new applications without the prior approval of the Technology Coordinator;
- Updating of existing applications without prior approval of the Technology Coordinator;
- Use that may result in the potential for data breach or the loss of District, student or employee records or data;
- Downloading games without prior approval of the Technology Coordinator;
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses or other malicious software and changes to hardware, software and monitoring tools;
- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks, or any communication that could reasonably be construed as racist, sexist, abusive or harassing to others;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and possibly destroyed.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or District web site unless the appropriate permission has been verified according to district policy.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

The district has selected an Internet filtering program, which has been installed on the district's network. This software protects against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of electronic/digital devices with Internet access by minors - harmful to minors. Website-specific exceptions to blocking shall be granted for the purpose of engaging in bona fide research related to an academic or co-curricular program or activity of the district, and only to the degree necessary and for the period necessary for conducting that research. The temporary access shall be enabled by the Technology Coordinator or his/her designee. If a student requests access, the Technology Coordinator or his/her designee shall initially review the site for appropriateness, after which the student's teacher must give prior approval before access is provided by the Technology Coordinator or his/her designee. If a staff member requests access, the

Technology Coordinator or his/her designee must provide access.

The selection of which websites are blocked, or exempted from blocking, shall be conducted fairly. Care shall be taken to ensure that a broad variety of views are available for student access, and to ensure that there is no bias – intentional or inadvertent – in the application of restrictions on access, especially in relation to controversial issues or political positions.

Any attempt to defeat or bypass the district's Internet filtering system or conceal Internet activity is prohibited, and will result in suspension or revocation of permission to use the district's computer network or Internet.

The fact that the filtering technology has not blocked access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the filtering software has blocked access to certain material shall not create the presumption that the material is inappropriate for users to access.

Users are responsible for the information they communicate across the network. This includes but is not limited to the disclosure of personal contact information (without specific building administrative approval).

Teachers or other staff members recommending or assigning the use of online services by students must verify in advance that the service has adequate measures in place to maintain student safety and privacy.

Downloading, copying, duplicating and distributing software, music, sound files, movies, images, intellectual property, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and complies with district policy, and content is cited appropriately. All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

All users of the district's computers, electronic/digital devices and electronic network shall, as a condition for use, read Policy 4526.1-R, Acceptable Use Policy for Computer and Internet Access Regulation (the Regulations). Each user, and in addition in the case of a minor child the parent(s) or legal guardian(s) of the user, shall receive a copy of the Acceptable Use Contract for Computer and Internet Use ("AUP Contract"), which must be signed and returned to the district on or before October 1st of each year. Individuals who do not return the signed AUP Contract by October 1st shall be blocked from access to the district's computers, electronic/digital devices and the Internet. A signed AUP Contract shall be submitted by each student user in Kindergarten through 4th grade, 5th grade, and 9th grade at the beginning of the school year, or at the time of entry into the school district if a student enrolls after the commencement of the school year.

The Regulations set forth examples of prohibited conduct and contain certain cautionary information that will help the user use the internet properly and appropriately. These Regulations define and explain policy violations and set forth the respective responsibilities of the district and the user.

The Superintendent shall be responsible for ensuring that appropriate instruction is provided at each grade, annually, as to the district's acceptable use policy; conduct that is prohibited under the acceptable use policy; proper "netiquette" expected of users of the district's computers, electronic/digital devices, and network. The Superintendent shall be responsible for ensuring that appropriate instruction and training is provided to every employee of the district as to the district's acceptable use policy; conduct that is prohibited under the acceptable use policy; proper "netiquette"

expected of users of the district's computers, electronic/digital devices, and network.

Communication through the Internet or the district's networks, however, is not considered private and there should be no expectation of privacy regarding any computer use of school district computers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Network administrators may remove or delete files, material and/or communications that are violative of district policy.

Students using a personal computer or personal electronic device on school property or during a school sponsored or related activity are subject to the rules and regulations regarding acceptable use in district policies, administrative rules, and federal and state law. Any use that is in violation of the foregoing may result in the student no longer being allowed to bring his/her personal electronic device onto school property and/or other disciplinary or corrective action in accordance with the Code of Conduct. By bringing a personal computer or personal electronic device onto school property or to a school sponsored or related event and/or connecting a personal electronic device to any technology resource of the district, the student consents that an authorized staff member may, if he/she has reasonable suspicion that the student has engaged in activities with such personal computer or personal electronic device that are inconsistent with this policy, any other policy of the district, or federal or state law, may confiscate said device and search the electronic device in a manner and to an extent that is consistent with and limited to the basis for the reasonable suspicion in order to determine whether a violation of district policy and/or federal or state law has occurred.

The district makes no guarantee that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.

The district is not responsible for the accuracy or quality of the information obtained through or stored on the network. Each user is responsible for verifying the integrity and authenticity or the information that is used and provided. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

The Superintendent will be responsible for maintaining a process for the dissemination of this policy to ensure that it is known and understood by staff and by students and their parents and guardians. This shall include an annual dissemination and review by teachers of age-appropriate Internet information and guidelines with all students; inclusion of this policy in all student and parent handbooks; written dissemination of the policy to parents; posting of the policy in computer laboratories, on the district website, and display upon login to the district network; discussion at parent "open house" nights; and other such measures as the Superintendent may determine.

Ref:

Cross-ref:

4500, Instructional Resources

4526-R, Acceptable Use Policy for Computer and Internet Access Regulation

4526-E, Acceptable Use Contract for Computer and Internet Use

4526.1, Internet Safety

4526.1-R, Internet Safety Regulation

4810, Teaching About Controversial Issues

5300, Code of Conduct

8635, Information Security Breach and Notification

8635-R, Information Security Breach and Notification Regulation

8650, School District Compliance with Copyright Law

8650-R, School District Compliance with Copyright Law Regulation

Adoption date: March 12, 2015

Revised: June 15, 2017

Continued without change: July 9, 2019

Croton-Harmon Schools
